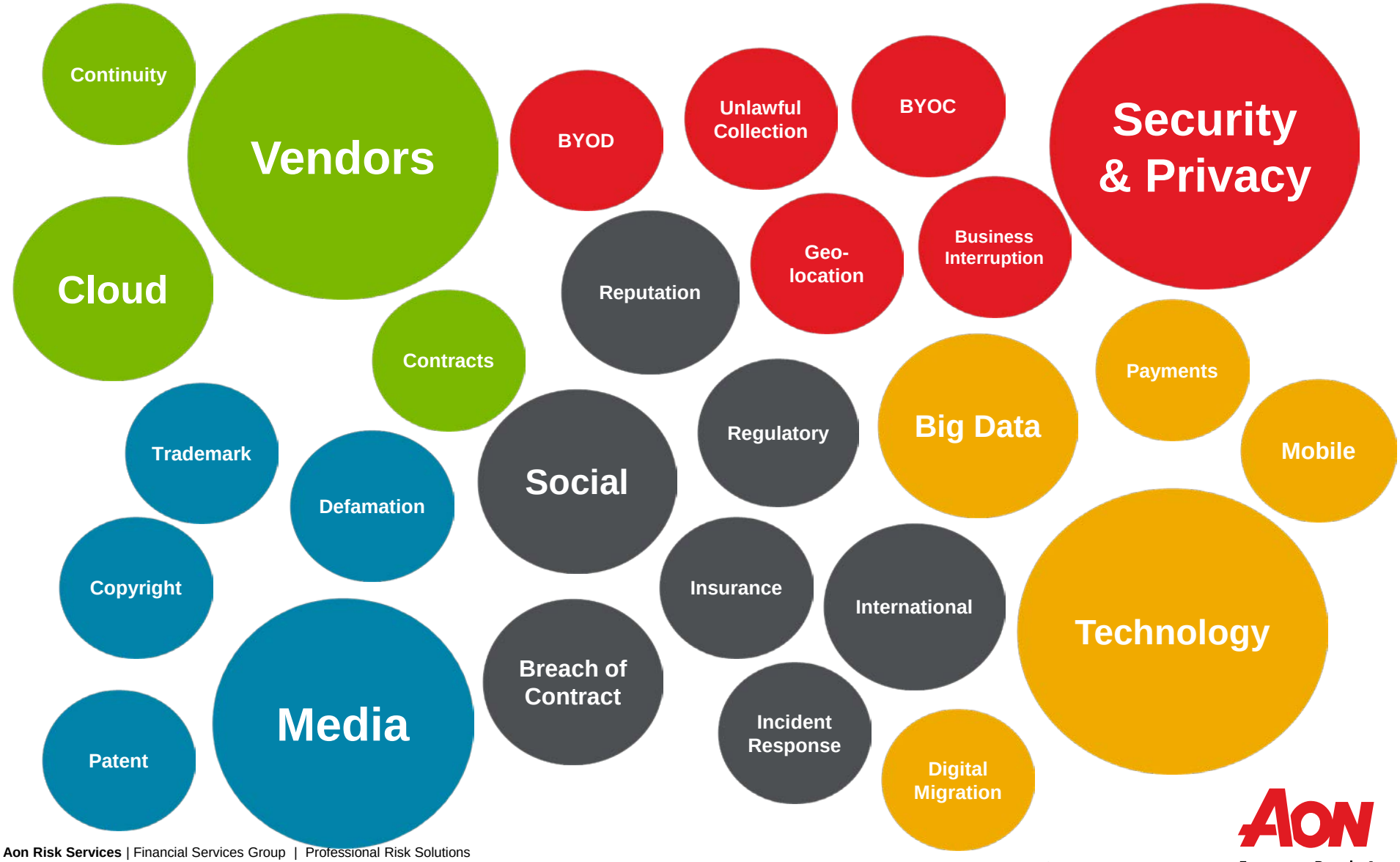
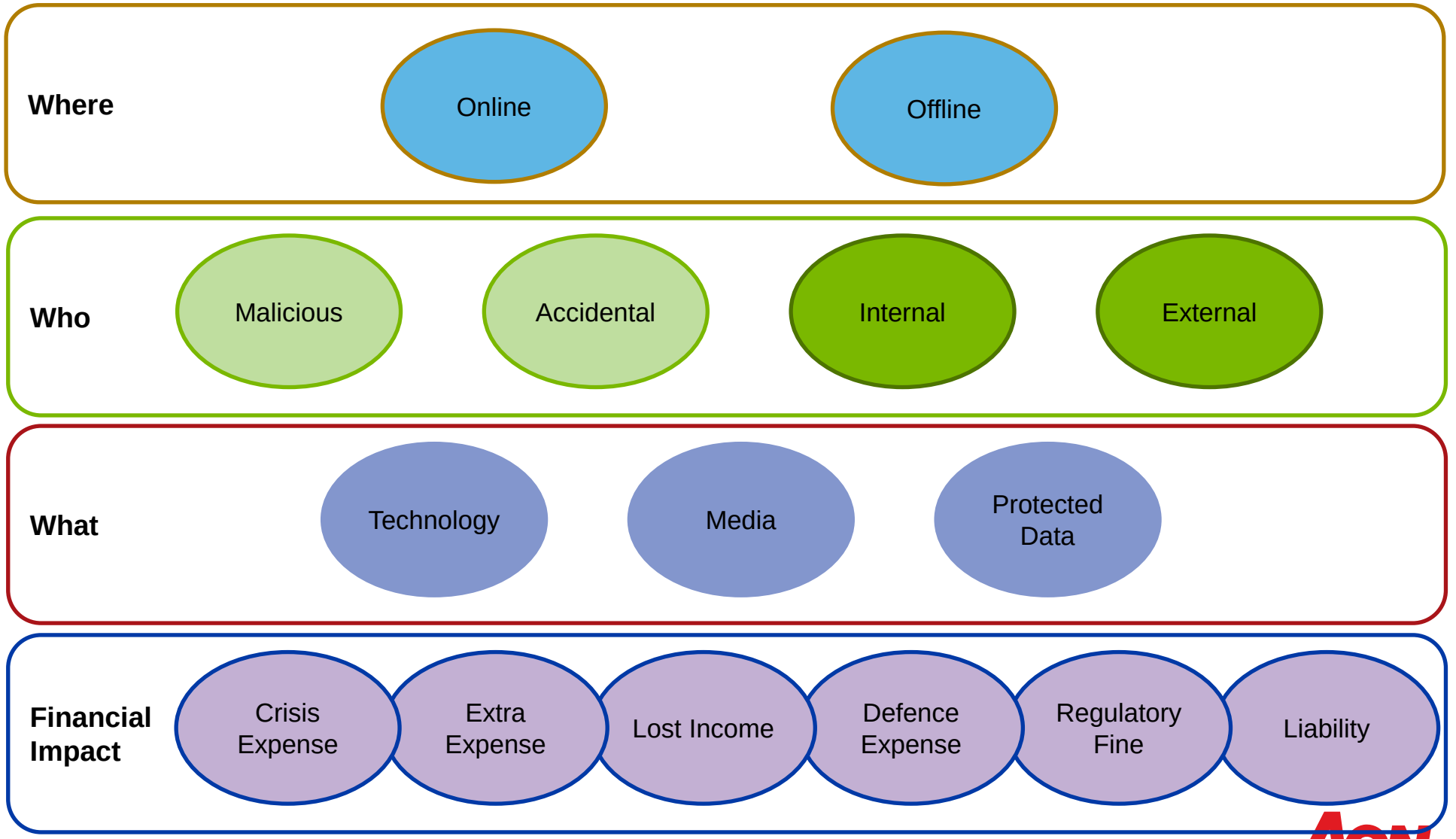
# Cyber Overview

# Scope of Growing & Emerging Threats

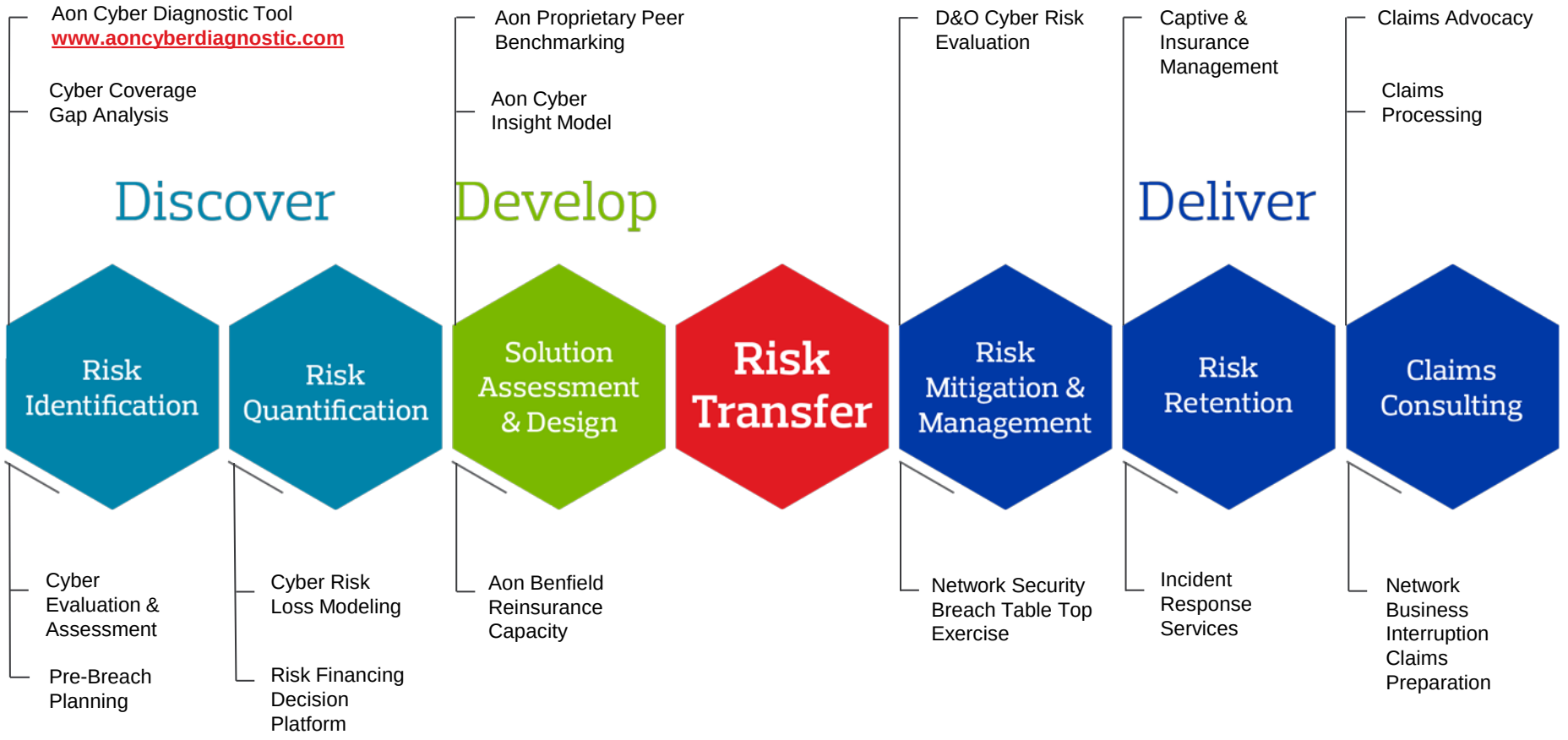


# What is Cyber?

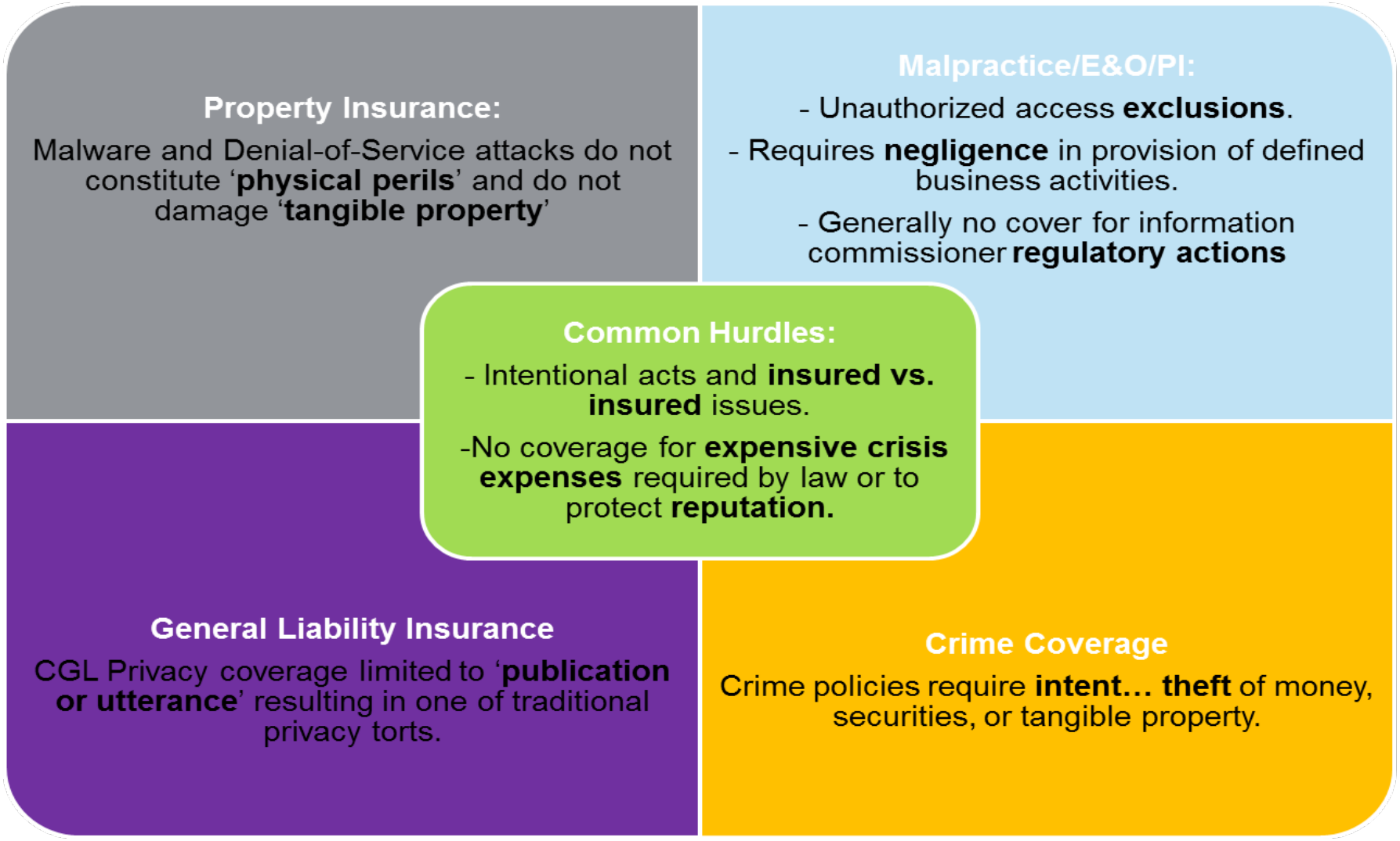


# Risk Discovery Process

# Aon Cyber Solutions Framework



# Legacy Insurance Coverage



# Scope of Cyber Insurance Coverage

## Third Party Liability Sections
*Defense Costs + Damages + Regulator Fines*

- ✓Failure of Network Security
- ✓Failure to Protect/ Wrongful Disclosure of Information, including employee information
- ✓Privacy or Security related regulator investigation
- ✓All of the above when committed by an outsourcer
- ✓Media content infringement/ defamatory content

## First Party Sections
*Insured's Loss*

- ✓Network-related Business Interruption
- ✓Extra Expense
- ✓System Failure Business Interruption (some policies)
- ✓Dependent Business Interruption (some policies)
- ✓Intangible Asset damage

## Expense/Service Sections
*Expenses Paid to Vendors*

- ✓Crisis Management
- ✓Breach-related Legal Advice
- ✓Forensic Investigation
- ✓Breach Notification
- ✓Call Center
- ✓Credit Monitoring, Identity Monitoring, ID Theft Insurance
- ✓Cyber Extortion Payments

# 3rd Party Coverage Elements (Triggered by a claim)

## Errors and Omissions Liability

Coverage for defense costs and damages suffered by others resulting from any actual or alleged negligent act, error, or omission committed in the conduct of in the performance of Professional Services.

- **Technology E&O:** Coverage for damages and defense costs for actual or alleged negligent act, error, omission, breach of duty or misstatement committed or omitted in the performance of your technology professional services to others.

## Security Liability

Coverage for defense costs and damages the insured is legally obligated to pay resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, and unauthorized use, denial of service attack or transmission of a computer virus.

## Privacy Liability

Coverage for defense costs and damages suffered by others for any failure to protect personally identifiable or confidential corporate information, whether or not due to a failure of network security. Includes unintentional violations of your privacy policy and misappropriation that results in identity theft.

## Privacy Regulatory Defense, Awards & Fines

Coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Coverage is typically sub-limited and may include (depending on insurer) coverage for fines and penalties to the extent insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered at full limits depending on the insurer.

***This is a summary of coverage, please refer to actual policy language for coverage afforded in the policy***

# 3rd Party Coverage Elements (Triggered by a claim)

## PCI DSS Fines and Assessments

Coverage for defense costs for investigations brought by the Payment Card Industry in connection with a failure to protect private information and/or a failure of network security that may have resulted from being non-compliant with PCI DSS. Coverage is typically sub-limited and may include (depending on insurer) coverage for fines and penalties.

## Network Extortion Coverage

*Triggered by a threat to cause a security failure or privacy breach*

Reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat. Payments are generally subject to full discretion by insurer.

## Media Liability

Coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured's website only to all content in any medium.

***This is a summary of coverage, please refer to actual policy language for coverage afforded in the policy***

# 1st Party Coverage Elements (Triggered by a breach)

## Data Breach Response and Crisis Management Coverage

Reimbursement for the insured's costs to respond to a data privacy or security incident. Policies are triggered either by the discovery of such an event, or a statutory obligation to notify customers of such an event. Covered expenses can include:

- Legal Expenses
- Computer Forensics expenses
- Public relations firm expenses and related advertising to restore your reputation
- Notification to consumers
- Consumer credit monitoring services

## Network Business Interruption

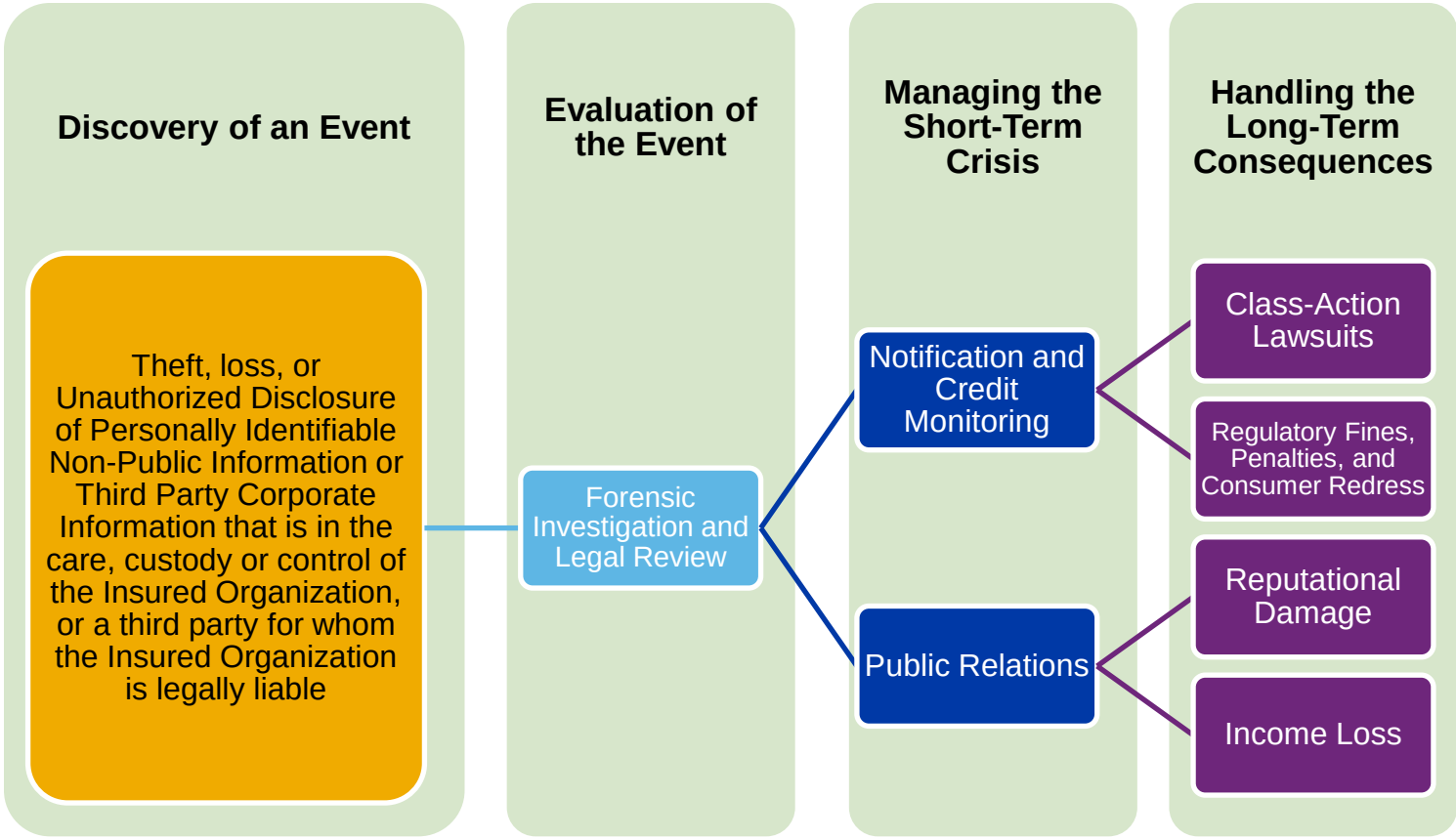
Reimburses the insured for actual lost net income and extra expense incurred when the insured's computer system is interrupted or suspended due to a failure of network security. Dependent Business Interruption is also available, but often subject to a sub-limit. Additionally, System Failure coverage is available upon request which provides limited coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security. In addition to a dollar amount retention, a waiting period retention of between 10 to 24 hours applies.

## Data Recovery

Reimburses the insured for costs incurred to restore or recollect intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a covered computer network security failure.

***This is a summary of coverage, please refer to actual policy language for coverage afforded in the policy***

# A Simplified View of a Data Breach Response Methodology

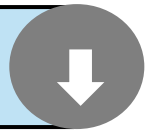



**Liability chain can vary depending on the nature of business & contracts**

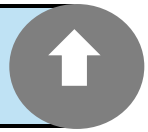
- If vendors are utilized for key IT or Payment functions, liabilities for breach events should be addressed via contract provisions

# State of the Market

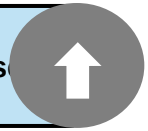
# Network Security & Privacy Liability Market Update

**Capacity** 

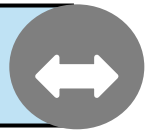
- **While the capacity for Cyber coverage remains stable with increasing competition in the middle market space, carriers are starting to pull back writing in certain classes of FI, Retail and Healthcare (Managed Care)**
  - Many carriers are non-renewing/pulling back capacity for companies with over $1B in revenue, specifically for retail, healthcare and FI companies
  - Markets exist domestically (primary and excess), the UK (primary and excess) and Bermuda (excess only)

**Coverage** 

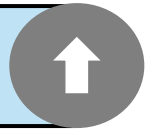
- **Coverage continues to expand in both breadth and limit availability for most organizations, except large FI, retail and healthcare**
  - Carriers continue to differentiate their offerings with new/enhanced coverage components (Breach Response Services, PCI Coverage, System Failure Business Interruption, etc.)
  - Carriers are willing to develop unique terms and conditions for difficult E&O risks, but require additional information

**Claims & Loss** 

- **Better data is being gathered as more breaches are reported, but still coverage cases regarding GL, Crime and Property**
  - While there is a large focus in the retail space, there continues to be numerous breaches reported with additional reports tracking costs of the breaches for FIs
  - Policies are responding, particularly to the breach mitigation, allowing better tracking of “claims” payments

**Retentions** 

- **Retentions remain stable and varied, but some large increase for accounts considered “high risk”**
  - Retentions of all levels are available in the market, but vary based on industry class, revenue and unique exposures—there have been some material increases for FIs, retail and healthcare in 2015 (double or triple)
  - Adjusting retentions can lead to more coverage/sublimit flexibility (trade-off for insureds)

**Pricing** 

- **Pricing continues to trend upwards**
  - Pricing continues to rise in the wake of significant breaches, particularly in the currently/expected to be affected industries such as financial institutions, healthcare and retail
  - Renewal premiums continue to increase between 15–20%+ for insureds with no change in exposure profile

# What to Ask

**WHO ARE THEY?**

**WHAT DO THEY DO?**

**WHAT COULD GO WRONG?**

**HOW DO THEY MANAGE THE EXPOSURE?**

**WHAT DO YOU WANT TO DO?**

# Cyber Environment Challenges Increased Underwriting Scrutiny

**How much personally identifiable information do you store, process, or maintain?**

| | Top Concerns |
|---|---|
| **High Volume of Credit Card Transactions** | - End to End Encryption?<br>- Tokenization?<br>- File Integrity Monitoring?<br>- Adequate compensating controls?<br>- Target dates for implementation? |
| **Reliance on Vendors** | - Outsourcing payment processing?<br>- Does the vendor hold the token key?<br>- Do you engage a third party to administer employee benefits?<br>- Limitations of Liability required within contracts?<br>- Additional Insured status required within contracts? |
| **Collection/ Maintenance/ Storage of PII** | - Are networks segregated by region?<br>- 2 Factor Authentication?<br>- How is employee information stored/ protected?<br>- BYOD/ BYOC?<br>- Data retention policies? |

**Combined effort between Legal, IT and Risk Management**

# Submission Considerations

- Fully Completed Mainform Application
- Financials
- Loss Runs with Details (if insured has current coverage)

MPL/Tech/Media:

- Master Service Agreement

Cyber:

- PCI Report on Compliance (if applicable)
- Underwriting Meeting